HIT Policy Committee
NHIN Workgroup
Draft Transcript
May 10, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, and welcome, everybody, to the NHIN Workgroup. This is a public call, and there will be opportunity at the end of the call for the public to make comments. Let me do a roll call now. David Lansky?

David Lansky – Pacific Business Group on Health – President & CEO
Yes. Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Neil Calman? He's on.

Neil Calman - Institute for Family Health - President & Cofounder
Yes, I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Jim Borland or somebody from Social Security? Christine Bechtel?

Christine Bechtel - National Partnership for Women & Families – VP
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Tim Cromwell? Marc Probst? Marc Overhage?

Marc Overhage – Regenstrief – Director
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Collin Evans? Arien Malec?

Arien Malec – RelayHealth – VP, Product Management
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Jonah Frohlich?

Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Leslie Harris? John Blair? Farzad Mostashari? Doug Fridsma? Mark Frisse? Joy Pritts?

Joy Pritts – ONC – Chief Privacy Officer
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Andrew McLaughlin? Latanya Sweeney? Connie Delaney? Adam Green?

Adam Green – Progressive Chain Campaign Committee – Cofounder
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anybody off that list? All right. With that, I'll turn it over to David Lansky.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks, Judy. Good morning, everyone. Welcome back. We've had a lot going on, and particularly, I think, the NHIN Direct work has been proceeding very rapidly under Arien's guidance. And I appreciate Arien being available this morning to walk us through an update of where NHIN Direct work is going and is to date. That will, in turn, tee up our discussion. The primary focus today is considering how the preliminary work we've been doing on the trust framework broadly fits with the work underway on NHIN Direct, and make sure we identify any areas that need additional discussion and attention that might be emerging as the NHIN Direct strategy starts to play out.

I know many of you have seen the slides that Mariann prepared to guide our discussion today, and that, in turn, teed up some questions several people raised about the framework itself, so I think we'll probably, in the course of coming to looking at the structure of the review of NHIN Direct policies, that will probably tee up some questions for us about our overall way of articulating the framework, so we'll come to that as well. First, unless I missed anything, Mariann, we'll let Arien kick us off with an update.

Mariann Yeager – NHIN – Policy and Governance Lead
Yes. That sounds great, David.

David Lansky – Pacific Business Group on Health – President & CEO
Arien, thanks for being here.

Arien Malec – RelayHealth – VP, Product Management

Absolutely. Thank you. I can only attend the first hour. I've got a flight that's going to take off in a bit, but Mariann and I have synched. I would love to stay for the trust … discussion, but I think Mariann knows everything that I do and more relating to the policy implications for NHIN Direct.

I just wanted to give you all an update as to the progress to date. We've been running for a little over two months with the NHIN Direct project, so if you can go to the next slide. Just definitionally, the project is a project, so it has a beginning and an end. The goal of the project is to create a set of standards and services that will, within a policy framework, and that policy framework is, you know, the NHIN Direct project is a technology project, not a policy project. So we're reliant on this group and the HIT Policy Committee in general, as well as the ONC policy office and other policy apparatuses to create the appropriate policy framework for the standards and services.

Again, the project is to create the standards and services that, within a policy framework, enables simple, direct, routed, scalable, transport over the Internet to be used for secure and meaningful exchange between known participants in support of meaningful use. And I've thrown in a bunch of adjectives there—simple, direct, routed, and scaleable—because I think the early, the orderly way we described this, and I think that when I was part of the NHIN workgroup, we were pretty clear about the role of intermediaries and the critical policy issues of intermediaries. I'm not sure that message got out and that we did a very good job in the early part of the project to describe the connectivity in a way that made it clear that trust enabling organizations were part of the overall trust fabric and part of the overall policy fabric. This is definitionally what we're at. The project will end with essentially paper artifacts or electronic equivalents to paper artifacts with some additional work on top of that, and we'll get to that in a second.

If we go to the next slide, what I did here is, and members of the HIT Standards Committee have seen, I think, pretty much this slide, which confused some people and clarified other people, so I'm not sure if that's – it's like the art of a good compromise. The goal here is to essentially say, you know, we've got a set of services on NHIN, and many HIOs have also taken that same set of services and used it to create essentially the RHIO or the state HIO architecture. And what about the NHIN Direct projects? What about this use case is new? And so we tried to basically put the two architectures side-by-side.

I think the one piece that I think is most compelling in the NHIN Direct overall approach is, A, that it's direct and routed, so it goes from someone to someone else, that the information holder is the transaction initiator, and that it encompasses the two endpoints of transactions. So if you look at the bottom of the slide, or the top of the slide in green are the NHIN Direct transactions, at least as we're thinking about them. The bottom of the slide in black are the current sets of transactions, the record locator model of transactions, although there is a pushed transaction. But all those transactions are node-to-node and deliberately leave off the edge of the connectivity. That's an overall overview for how these two orchestrations both fit together and are different. As I said, the new thing about NHIN Direct primarily is the addressing and routing that enables the direct connectivity between two endpoints.

One point of clarification that is confusing about this slide, or it may not be the only thing that's confusing about this slide is that this upper bit of the HISP address directory, if you read it as a HISP address directory, so HISP is what we're calling the trust enabling organizations from a technology perspective or the routing organizations from the technology perspective. If you read that as an address directory that's hosted by the HISP, then it looks like it's a place to look up information about endpoints. That's actually not its function at all. It's the HISP address directory, so it's a place to look up the address of the other routing party. If you're sending information from doctor A to doctor B, doctor A's routing function needs to

know where doctor B gets routed to and needs to be able to look up that. Generally that's going to be the plain old DNF that will be the HISP address directory.

If we can go to the next slide, I'll go quickly through this, and then we can do some discussion. There are a rather large number of organizations that have made levels of commitments to the project. Generally levels of commit to the project that have been made are either to create some open source technology or to host real world implementation or both. And we'd got some 40-some organizations that have made that level of commitment to the project. And we've gotten, I think, really good participation and involvement through the process through a set of implementation work meetings, as well as a whole set of workgroup meetings, and we just concluded. At the end of last week, we concluded our first face-to-face meeting to get together and explore a lot of the technology implications or what it is that we've been working on.

If we can go to the next slide, we've put together a rather aggressive timeline, and the reason for being so aggressive is primarily because we want to see real world implementation of the kinds of direct transactions that we're talking about in 2010 so that we can learn from them and then roll them out in wider scale in 2011 in order for it to be meaningful, as it were, for meaningful use. And so what I've done here is taken the overall calendar toward the September/October timeframe where we'll get the first real world implementation up and running, and then noted the kinds of deliverables that we're looking for. We just had our face-to-face meeting, as I noted.

We got part of the way through our first draft specification. We've got a little more work to do, primarily focused on natural coding work that's going on, which is, as usual, getting real about this stuff exposes a lot of issues that we're working through. We're marching towards a couple of really concrete milestones in June, as well as in July. In June, we're hoping to get specifications finely detailed. Then, in July, the whole rest of the apparatus around the support structure for development organizations up and running, including reference implementations, testing frameworks, and then the whole host of documentation that helps developers get up and running in order to, as I said, get really real with actual providers in September/October.

Now there are a lot of things that need to happen, both from a technology perspective and a policy perspective to make that latter timeline realistic and work. We're trying to do the right level of coordination to get there. I think it's fair to say, we've been moving awfully quickly and need to be better about meetings like this to basically synch back with the policy-making folks.

If you go to the next slide, the deliverables that we will exit this project with include both formalized models and textual descriptions of the core specifications and service description. That's really the primary deliverable. There's a whole set of testing artifacts or conformance artifacts, conformance testing scripts and the conformance service. Then a set of packaging or information to assist developers in being able to write to the specifications, so my experience is the dry specification is great if you actually know what it means. And sometimes you need some documentation that goes around it, and some of that documentation will include executable code in the form of open source projects that people can take off the shelf and use, as well as additional documentation.

Then there's a whole set of additional deliverables that we'll have. One is the actual process that we've used for NHIN Direct, what's worked, what hasn't. Is this a good model for standards development? Is this a bad model for standards development? What can we use out of this project to better inform the overall process? I know that the work that we've been doing to date has been helpful in framing up some thinking inside ONC about the standard interoperability framework and how ONC and the HIT Standards Committee catch standards that are under active development.

The NHIN Direct project itself does not drive or frame or create any policy recommendations, but there is a strong technology policy intersection, interaction, and we've tried to frame up or tee up a number of the key policy issues that we are running into from a technology perspective, and we'll talk in just a second about how it is that we've been reporting out those teed up policy issues for the consideration and what I think we can do a better job of after that. Then standards and specifications, in my experience, are half technology and half awareness, and so there's a whole set of marketing and awareness deliverables that we expect to the extent that the project itself is successful. Again, I want to emphasize that we're two months into the project. We've got a bunch of good work that's been done. But we're going to actually have to see some real world stuff before we actually start talking about it from a marketing perspective.

You can go to the next slide. The working groups that we have up and running currently, we've got a user story review working group that's really tasked with essentially mapping primarily meaningful use criteria from a clinical perspective to the kinds of process flows and technology flows that we're looking at from a technology perspective. We've got a concrete implementation working group that is essentially tasking teams or working with teams that actually are doing real world coding right now, essentially testing out some of the concepts we've been talking about from the rest of the working group. The content packaging working group is talking about how do you take. You know, we're trying to stay content neutral, but how do you actually take the actual health content and package it up for further delivery.

Security and trust is primarily a technology working group, but this is the working group where we've got a strong policy/technology intersection. And we've been, you know, this group has been primarily looking at technology enablement of policy. We've been trying to plug the output of this work into the privacy and security workgroup of the policy committee, as well as this workgroup. Again, we'll talk in a second how well we've been doing … plugging into and what we can do a better job of or how we can do a better job of that in the future.

I also want to make it clear; this is the security trust working group from a technology perspective, not from the policy perspective. But as I said, this is one of these areas where things are so tightly intertwined that it's really hard to stay at a policy. This group basically presented its work at the face-to-face, and we'd invited Deven to that meeting, and her first comment was, "I see 15 different policy implications from this policy neutral statement that you made," just as a way of pointing out how hard it is to separate policy and technology in this area.

Robust, or now we call it comprehensive HIE interoperability. It's essentially looking at the NHIN Direct services and the current NHIN services, and making sure that they harmonize to scale. Individual involvement, so what's the role of the individual or the patient in the process, and how can the work that we're doing from the technology perspective extend out to patients and other individuals?

Implementation geographies is looking at, we really have a goal of testing this in the real world, so what are the right geographies for doing that testing? And what kinds of things from a process perspective do we need to think about to run a real instance of this in the real world? Addressing looks at what is the form of a health Internet address and in a way that can be further used in, for example, addressing directories or used to plug into somebody's EHR in order to route or send a message to another provider.

Then our abstract model is essentially our technology neutral description of all of the services that we have available. All of the output of these working groups is publicly available on the nhindirect.org Web site. I will admit that there's a ton of content that's out there, so it's sometimes hard to wade through. But we've been trying to do a reasonably good job about keeping everything in the public eye.

If you can go to the next slide, that's it. I thought we had one more slide. The last slide that I do want to talk about is how we plug the work that we're doing into the policymaking organization such as this workgroup. Internal to ONC, we've got two mechanisms for synching the work that we're doing up with the key policy folks.

One is a weekly steering team meeting. The key participants actually are on this workgroup: Farzad, Todd, and Doug and Andrew. Andrew McLaughlin is the key sort of internal to the government steering team for NHIN Direct. We also have a couple of policy steering meetings. One is with Jodi, Joy, and Mariann, and then we try to meet a little more frequently with Mariann just to make sure we've got good policy coordination internally.

Then there are two HIT Policy Committee connection points that I think we need to be doing a better job of staying in synch. One is with the privacy and security workgroup of the HIT Policy Committee, and the other obviously is with this working group. With privacy and security, I met with Deven last week, invited her to our face-to-face meeting, and we're talking now about how to get better plugged in to the work that she's doing and her workgroup, that that workgroup is doing, and then, as I said, I'm open to talking about how to get better plugged into this workgroup and make sure that we're providing the right hooks into the policymaking or discussing arenas out of the technology.

With that, I'm going to open it up. I tried to go pretty quickly through it. I'm going to open it up for QA.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks, Arien. Yes, let's just see if people have some immediate questions before we get into some of the detailed policy implications of the model. No. Everyone is content. Thank you for doing the presentation.

Arien Malec – RelayHealth – VP, Product Management
Absolutely. Thank you.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
This is Carol. Can I ask a question?

David Lansky – Pacific Business Group on Health – President & CEO
Please.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Two things: first, the comment you made earlier about the intermediaries and sort of a correction that intermediaries are required. You use the term trust enhancing organizations. And I've been pleading the case for trust enhancing functions for a long time because I think the implication of organization is not only that you sort of – the trust comes from an outsourced party, but also that there's some expected bundle that organizations are going to offer. And I don't think we know what that bundle is. I think it could vary depending on the participants, so I'd be much more happy if we could not imply that it's an organization necessarily that's going to be playing all of the potential functions that might fight into the trust framework. That's my comment.

But my question is really, I noticed on the slide, you have security and trust specifications that are coming out in May. Looking at the composition of who is participating in NHIN Direct, I'm wondering where those specifications … which workgroup is supposed to look at those? I guess it's more a general question also about where you're getting the policy input for that.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
This is Farzad. Let me jump in here. At the all-day meeting, I pointed out to the group that the challenge was going to be to stay within the policy bounds that were defined by the NHIN workgroup and discussed by the privacy and security workgroup, which is the direct transmission of information for treatment purposes or other HIPAA – non-disruptive HIPAA blessed approaches when it comes to patient consent, certainly, that we have discussed in this workgroup for some time now where the enabling, and adding the caveat that was pointed out by the policy privacy and security workgroup that the enabling organizations within the architecture need not have access to personal health information. That is the policy … where essentially we are improving on existing methods of sending information from one place to another without any – as far as anyone, I'm aware, has been able to identify any potentially disruptive privacy or policy concerns.

The work of the security, and I think part of it has been, and we pointed out this out, and I think we've got an acknowledgement that the NHIN Direct group has to do a better job of using the same language that has come from the NHIN workgroup and the privacy and security workgroup to talk about things. But their security workgroup or committee or whatever, this has really, from a technology point of view, they're trying to figure out. We gave them the mission to make sure you have mutually authenticated, encrypted, secure routing from point A to point B. Essentially what they're trying to figure out is, is that going to be accomplished by having certificates at the centrally managed certificates at the edge, or is this going to be TLS with the subsequent server to or hit to clients interactions be the responsibility of the hit.

That's the technical issue that they're wrestling with things about whether it is feasible to have static IPs and TLS certificates at the edge or not. It is not, I believe, as far as I've been able to tell and conform, and we've been looking for it, anything that makes any disruptive policy, preemptive policy decisions. If you have any specific concerns, I think we really, we do want to and need to have a tighter connection between the policy work and the NHIN Direct work.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I understand that we're saying intermediaries don't have PHI, but I'm assuming they have identifying information.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
About the patient?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Or the provider. In other words, what's the policy? What are the policies that will guide the sort of trust for those organizations? Who is developing the criteria for whether or not their government is going to say they are being trustworthy?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
We are. You are. That's what we were trying to get the NHIN workgroup, the work over the past few sessions has been to get down to the level where we can say for those specific functions who the governance over those functions are going to work. And we discussed on the last call that there's a belief that there needs to be governmental, indeed federal oversight over organizations that provide those functions. Maybe there are multiple organizations that provide different functions; maybe some organizations provide multiple functions. But what we need to get to now is more specifics around what would be the requirements for enabling trust in those organizations and the regulations that might be required. Ultimately, our goal is for this workgroup working with the privacy and security workgroup to get

to the point where we can define in some detail what the specifics are of what are going to be the criteria for making sure that those organizations can be trusted.

David Lansky – Pacific Business Group on Health – President & CEO
Farzad, this is David. I'll ask Arien or you if you could, maybe going back to the diagram that was your third slide, I guess, Arien, can you characterize for us, as you're going through these different scenarios and use cases, the functions that the HISP address directory needs to handle? Following Carol's vocabulary distinction in talking about functions rather than organizations, help us understand what are the functions, which ones imply organizational capability or certification of an organization, etc.?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Again, David, I'll say that this work is completely derivative of the work that the NHIN Direct workgroup has done. I think, if you look at our previous presentations from the NHIN workgroup or what you presented to the policy committee, it comes from there, so those are the secure routing function, the identity assurance function, which has not been discussed yet by the NHIN Direct group. And we talked about the question of whether directory services are required or not and that's an issue that the NHIN workgroup has yet to tackle in terms of whether that's a third or whether we do need to have governance over those directory services or not, but this is all from the work that the work that the NHIN workgroup has done. I think, the problem with the NHIN Direct workgroup has been lack of overt direct reference to the guidance from this workgroup, but it's not because it's not there. I think it's more stylistic than anything.

David Lansky – Pacific Business Group on Health – President & CEO
What I'm asking actually is, I think it's useful for us to have NHIN Direct going through the detailed work that it's going, which is far ahead of the level of specificity that we've been at as a workgroup here, and that provides a good vehicle for us to ask some questions about whether the framework we've begun to sketch at a high level is going to be adequate to address some of the requirements on the ground that are being elaborated now with the Direct program.

As a layperson, what I'm observing is that the flushing out of the NHIN Direct program, as Arien sketches it, begins to touch upon more of the policy issues than I had imagined two months ago it would when I understood NHIN Direct in a very simpleminded way. And maybe it's just inevitable that we're going to surface a set of issues no matter which technical scope we undertake that take us to the same set of questions that we need to answer with the policy security group relatively faster.

Arien Malec – RelayHealth – VP, Product Management
That's a great way to put it is that the goal of getting to running code and rough consent is building prototypes is that they surface the policy issues. I think there needs to be an iterative process where, as the initial policy guidance is given, attempts to instantiate that technology identifies new issues. I think now we're beginning to be at the point where we can start to bring some of those back to the policy environment.

David Lansky – Pacific Business Group on Health – President & CEO
I suspect that's what'll happen in the second half of our discussion today. Arien, can I take you back to slide three and just have you, just for our benefit again, maybe elaborate a little bit on what those functions are that you see being needed by the HISP like service?

Arien Malec – RelayHealth – VP, Product Management
Sure. I can go back there. If we can move…. Excellent. I think a lot of the key services are really encapsulated by those three green arrows. This diagram presents a point of view where physician A,

physician B, and the routing functions are separate functions. I'd say they are separable functions. They can be combined. In some cases, it's illustrative to think about them as four potentially separate and distinct…. And so there are a couple of key points. Number one, as Farzad mentioned, there's identity assurance and authentication that precedes the send to the information and deliver patient information steps between the endpoints, physician A and her HISP, and physician B or the patient and his or her HISP.

Joy Pritts – ONC – Chief Privacy Officer
Arien, this is Joy. I have a question. When you say identity assurance and authentication, do you mean patient, provider, or both?

Arien Malec – RelayHealth – VP, Product Management
Both, and clearly there's a difference.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Can I speak in there for a minute? This is Wes Rishel. I would like to be very clear that identity of the patient, authentication identity of the patient is conceived here when the patient is interacting with the system. It's not the identity of the patient as conveyed in a document that is necessarily even available to the HISP. Is that a correct statement, Arien?

Arien Malec – RelayHealth – VP, Product Management
That's exactly right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I also want to highlight that although the members of this group, as well as the NHIN Direct group feel very strongly that we should look at how to deliver results to patients and how to enable messaging from patients to their providers because of the importance of that that we recognize explicitly that the challenges around identity assurance of patients, clients, members of the public are in order of magnitude probably more difficult than that of providers. So there hasn't been any, I think, specific progress in terms of how that's done other than to say that it would probably require some face-to-face interaction at the doctor's office the way it's currently happening with, say, a Google Health or Microsoft HealthVault. The patient, who is confirmed to be the patient at the doctor's office, giving an address where information can be sent.

Arien Malec – RelayHealth – VP, Product Management
And our motivating user stories actually explicitly mark that as a key assumption that prior to any transmissions, the patient, the information holder has confirmed to his or her satisfaction the identity of the patient. The second key piece of information or the second key role or function, to Carol's point, is the information routing function. Here, from a technology standpoint, there are a couple of things that we're trying to insure. Number one, we're trying to insure that the information that's required to route information, the header information is kept as fair and minimal as possible such that it's possible to encrypt the actual body content that contains personal identifiable health information. And insure that the routing function need never see that information without explicit….

David Lansky – Pacific Business Group on Health – President & CEO
Arien, before you go further, can I ask you a question about it?

Arien Malec – RelayHealth – VP, Product Management
Sure.

David Lansky – Pacific Business Group on Health – President & CEO
The first arrow, I guess, and I don't want to overinterpret the visuals here, but the traffic going to this directory service or not, I'm trying to understand. Is the first action that doctor A is querying the directory for a precise address for doctor B, or does doctor A already know the address from prior trust relationships?

Arien Malec – RelayHealth – VP, Product Management
The assumption, yes, again, that's what I was trying to get at in my attempt to parse the words. It's a HIPS address directory, not a HISP address directory. The assumption is that provider A already knows provider B or patient's address out of band and that the function of the routing, the routing function is to find out from that address where that message needs to go. Then in that function of finding out where that message needs to go, we also need to insure in that leg of the transaction, that middle green leg of the transaction that the two endpoints that are being routed to are in the trust fabric, are in the trust network for the key participants.

But again, we're looking. We're keeping address directory lookups right now out of scope from a technology perspective. We may explore from a technology perspective how you do that. I also want to acknowledge that there are some additional policy considerations for maintenance.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes, and I think Wes has pointed out that we can start with internally maintained directors and the way we do with e-mails today, and there could be a migration to having kind of global directories available with universal addressing that's portable and so forth.

Leslie Harris – Center for Democracy & Technology – President & CEO
This is Leslie. Let me just make sure I understand something. In terms of the routing function, aren't we assuming that this is going over the Internet using the routing that is already there with the ISP?

Arien Malec – RelayHealth – VP, Product Management
Correct. The only reason to make this a generic step is that the NHIN exchange uses a different mechanism. They use a UDDI mechanism.

Leslie Harris – Center for Democracy & Technology – President & CEO
But here we're not, right?

Arien Malec – RelayHealth – VP, Product Management
We're assuming that we're using the DNS as our core routing.

Leslie Harris – Center for Democracy & Technology – President & CEO
I just want to make sure.

Arien Malec – RelayHealth – VP, Product Management
Yes. We're not trying to reinvent … technology.

Leslie Harris – Center for Democracy & Technology – President & CEO
Who these key areas are in that transaction….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If I could elaborate just a second, if it's okay. Arien, if you're not feeling supported here, let me know.

Arien Malec – RelayHealth – VP, Product Management
I'm among friends. It's good.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Because I can be quiet. It has happened once or twice. In addition to the domain name service, which would probably be an element of communication with NHIN Direct and would be the primary element of communication on other models, there is a little bit of additional functionality applied there in terms of assuring a higher level of authentication in encryption than is commonly used in the Internet.

Leslie Harris – Center for Democracy & Technology – President & CEO
Right, but isn't that function at the end? Doesn't each provider have an identity provider?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. That's why the abstraction that he's trying to convey here is a little bit – well, it's abstract. It covers some alternative opportunities. But it's likely that if digital certificates are being used, there is in the more elaborately played out version in the future, the one that comes after the initial work, there is some mechanism, whether that is strictly PKI or something else in the future that enables those endpoints to do that encryption for a broader population. One of the primary reasons this is confusing is that it seems to imply something besides direct transmission over the Internet, but in fact that's not. It's only enabling that securely that's going on there.

Arien Malec – RelayHealth – VP, Product Management
That's right. An additional point for the look up on the DNS, as Wes says, we're also using or assuming we're using digital certificates to verify the identity of the key parties to make sure that we're mutually authenticating, as well as doing the address lookup. So there's semi-sophisticated attack called DNS poisoning where you can fool the DNS to say this address actually points over here, and the solution to that from an architecture perspective is to make sure that when the two routing functions talk to each other, they confirm. Yes, I'm in the trust network, and I am who I am or who I say I am.

Leslie Harris – Center for Democracy & Technology – President & CEO
Who does that function of not just pointing through the DNS, but then confirming that?

Arien Malec – RelayHealth – VP, Product Management
From a technology perspective—

Leslie Harris – Center for Democracy & Technology – President & CEO
I guess I'm trying to figure out how many actors there are.

Arien Malec – RelayHealth – VP, Product Management
That's right. From a technology perspective, so there is a technology side to this and a policy side to this.

Leslie Harris – Center for Democracy & Technology – President & CEO
Right.

Arien Malec – RelayHealth – VP, Product Management
From the technology side of this, the answer is, we think, PKI and standard digital certificates. From a policy perspective, there's clearly the how do you get one of those? How do you establish that you're

inside the trust network? What do you need to do to get one of those? And I think that's the key work that….

Leslie Harris – Center for Democracy & Technology – President & CEO
That's what I think too that we're really talking about that bundle of identity related, getting and confirming. All right.

Arien Malec – RelayHealth – VP, Product Management
Exactly.

David Lansky – Pacific Business Group on Health – President & CEO
Let me ask either Leslie or Arien. Whose job is it to flush that out? Does it come to this workgroup or to the privacy and security workgroup, or will the Direct group begin to sketch at least the requirements there?

Leslie Harris – Center for Democracy & Technology – President & CEO
That was my question too.

Arien Malec – RelayHealth – VP, Product Management
We are, just to kind of keep roles and responsibilities clear, we're creating a mechanism by which once there's a policy framework that's been established, we'll have a technology means of expressing it. We'll have a technology means of saying we're both in the trust circle. But how I get in the trust circle is not a technology issue. It's a policy issue.

David Lansky – Pacific Business Group on Health – President & CEO
To me, just in terms of project management, when you look at your timeline that you sketched for us today, and the opportunity you have for some implementation trials, obviously afraid of the cart getting ahead of the horse here.

Arien Malec – RelayHealth – VP, Product Management
Yes. I'll let Farzad speak to this as well. There is another timing issue, which is that even if there was a federal role to play in insuring the process by which somebody becomes part of the trust circle, if you will, the timeline, even if this workgroup said here's exactly what to do, the timeline still doesn't fit. So we're going to need some interim process for the initial pilot. The other thing I'd note is that this kind of exchange work is being done today through private parties through individual trust, although I think we'd like to get something in between private parties through individual contracting and full scale, federally based policy. I'm going to flip that one over to Farzad.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I just wanted to hear more actually from David. I think he was going somewhere.

David Lansky – Pacific Business Group on Health – President & CEO
No. Where I'm going is just trying to get a charge to this group. If there is some work we need to do to be providing timing guidance to the technical side of NHIN Direct, and I think there is, and as we begin to see, understand better what the functional requirements are of this model, even this very short discussion today, we start teasing those out. I think we need a to-do list. Arien, before you go to your plane, I hope you can give us your top of mind to-do list for policy framework, how many layers we need to get how quickly so that we can begin to shape our tasks in the next couple months to make sure there's a deliverable that we come up with that's useful to the NHIN Direct implementation.

Arien Malec – RelayHealth – VP, Product Management
We've done some of that. I think the presentation that Mariann will walk you through has some of that thinking in it already.

David Lansky – Pacific Business Group on Health – President & CEO
Is there anything before you have to start running? Anything else you want to make sure we have on our radar, as we start this discussion today?

Arien Malec – RelayHealth – VP, Product Management
Just making sure that we've got a good coordination point, and I've actually got a request that I need to send out to you, to Deven, and to Andrew, a good coordination point between the two key policy workgroups to make sure that all three of us are at least aware of each other's activities and moving in the same direction.

David Lansky – Pacific Business Group on Health – President & CEO
Yes. I'm sure we can do that. I guess my worry at this point is since we'll come to this obviously in the next few minutes, we need an overarching framework within which we text the solutions you're working on to make sure that we're consistent with the goals that the policy framework lays out and that we've asked all the right questions during our charge. And I think we have a good start today with Mariann's material, and we'll come to that here shortly.

Even as we've talked in the first few minutes, it seems to me that I hadn't really expected a number of the issues your workgroup, the work team Arien has come up with, resurface some of the same issues that our overall group hasn't really wrestled with yet. For example, the role of the HISP, the identity assurance, whatever requirements are going to be imposed to provide that trust assurance across the parties. I thought we sort of obviated the need for some of that with NHIN Direct, and it sounds like we haven't, and that's probably very sound. We realize that now and understand what those policy guidance is that we need to come up with. We'll turn to that now, but let me just ask if people have any last questions for Arien before he has to take off.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
It's Farzad. I do want to point out a couple and, Arien, ask you to also think on your feet here. Listening to the discussions on the face-to-face and following a little bit the NHIN Direct blog, it seems like there were a couple of immediate issues that have floated up in terms of that may have policy relevance. Again, on some of those, I don't know that we can make some policy recommendations until we understand more in the prototyping phase what the complexities and issues are. One of them that struck me was the organization versus individual identity assurance.

Arien Malec – RelayHealth – VP, Product Management
Yes.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
To explain this as the technical folks started thinking through some of these practical implementation, it becomes clear that in at least some instances, you want the endpoints to be not a carbon based life form, but to be, for example, lab results at Sunset Family Practice. And that is a little mind bending for me in terms of how I identity assurance works at the organizational level.

I think, from a technical point of view, it's not a problem. They have a certificate. But from a policy point of view, I don't know I anyone has had experience with or can speak to this, but it would be interesting to explore that.

David Lansky – Pacific Business Group on Health – President & CEO
One other policy technology intersection point is that it's easiest from a technology standpoint if the certificate, so there's a question about in whose name the certificates are held. And it's easiest, from a technology perspective, if it's the routing functions that hold the certificate and that essentially they are taking on responsibility and a significant amount of responsibility to insure the other functions that are necessary for enabling trust such as identity assurance, including of non-carbon-based life forms, in some cases abstract life forms or abstract entities like a referral queue, authentication, and then there's a whole set of trust enabling functions around security audit, quality, those kinds of things.

It's easiest from a technology perspective if the holder of the assertion that these things have been done is done at the routing function because there's a lot of art for how to do that. It's harder if that assertion gets done in the name of the endpoint because it requires, in essence, an explosion of the PKI infrastructure and a lot of PKI technology work that is not new technology, but it's application of existing technology on a much larger scale. So that's an area where policy can make technology easier or harder.

Then the other one that I think Mariann is going to get into is what's the minimal PHI exposure that a routing function has, and then what happens as that PHI exposure gets higher? What do we need to make sure happens from a technology perspective in order to – first of all, what are our key assumptions from a technology perspective that we need to keep de minimus, at least from a requirement perspective. Then, as they hold gets a little relaxed, there's a whole set of policy implications that we need, I think, guidance for some of the initial work that we do.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
The other issue that came up that I thought was worthy of raising was the way the technology group is thinking about this is to build the architecture in such a way that it can instantiate various policy decisions. While in some instances if the policy decision is clear, the technology could be constrained so that it's embodied only that policy stance. I'll give you an example.

There was a discussion about whether the form and, Arien or Wes, you're going to have to help me out here, on the equivalent of an e-mail attachment, whether that had to be – that included a find mime message or whether it could only be a signed message. And on the one hand, clearly it enables the kind of mutual authentication encryption that we are talking about here, but the question is from a technology perspective. Should it also enable an unsigned transaction where the, for example, I don't know? It's a different kind of message. For example, there may be a text message where one provider wants to talk to another one about the golf game or whatever, whether they could use the same transport mechanism to send unsigned messages. We had some discussion.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm wondering if that relates to the discussion we had about using, building in this method, a way to authenticate what is a legal signature for a document conveyed digitally as opposed to the use of digital certificates and the technology that is called digital signature to insure the authentication and authenticity and encryption of the message. If it is the same thing, then that is, in effect, the equivalent to the things that Arien was just describing, although he was being broader and more abstract in his description. The thing that came up last week was that the final rule from FDA on narcotic prescriptions implies a level of PKI for individual signatures that wasn't necessarily believed to be practical before.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I'm not sure I followed all that, Wes, but I guess….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I was less concerned about an e-mail about the golf game than he was an e-mail that conveys a standard CCD or a CCR that indicates in the data that such-and-such a physician has signed a document versus one that conveys that signature through a mechanism like FDA uses for prescriptions that is unfakeable, in essence, or more difficult to fake for security reasons.

Arien Malec – RelayHealth – VP, Product Management
Just to try to frame up this issue, I think a lot of the key policy issues is in whose name does the trust assertion need to be made.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right.

Arien Malec – RelayHealth – VP, Product Management
I just want to surface this technology/policy tradeoff, which is that the lower down we go in the hierarchy of entities, the more difficult, the more assurance we have. We can express trust assurance down at the referral queue level or at the Dr. Smith level. But the more difficult the technology is that we're applying, on the other side, if we can express a level of assurance at the routing function only, we're creating that writing function and giving it a lot of responsibility in terms of trust assurance. But we're making the technology significantly easier because we've got existing….

There's a key policy issue about what level down that trust assurance needs to go, and the lower down it goes, the more certificates you have, the more signing you have, the more assurance you have, and the more complexity you have. There's a tradeoff there. As Wes says, the DEA rule has, in essence, already pushed that down some, not necessarily all the way out to the endpoint, but in many cases out to the endpoint. But it's already mandated for subset of providers that are doing scheduled medications who are going to need to wrestle with this particular issue.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
My understanding of the discussion at that group, and it's just my understanding was that through the allowance of the biometric provision that a provider could use biometrics and then have the token or certificate be at the organization level.

Arien Malec – RelayHealth – VP, Product Management
The organization level, right.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Not required now with the modified IFR that there be essentially PKI out to….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
But this also raises exactly the point that you have to push down as far as you can, but where you end up is also dependent on the other policies that govern this function. The other information policies, you know, what's retained, what's seen, transparency, accountability, oversight, all these things will play into how to look at some of these technical issues and should.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes. The third policy issue that I saw raised at the – so for me, the three were, to just be clear, the first was identity assurance at what level: organization, provider, and anywhere in between. The second was does the technology – is the goal for the technology to be constrained to he policy kind of specific policy

bound, or does it need to be enabling of a variety of policy decisions current and future, as a general issue? Then the third was, there's agreement that we don't want to get into the content at this stage, and that's kind of off bound, and that the header should not contain any personal health information, and that should be in the payload, and that to do this routing should not require anyone to look at the payload itself, should not require that.

The one, I thought, policy relevant question that came up was, however, whether the header should permit or allow assertions to be expressed regarding the compliance of the payload to certain standards, and the business scenario there is that certain organizations for liability or other reasons may wish never to even receive a piece of a message if they don't have an assurance that the content is correctly configured and compliant with the standard they're expecting. Clearly not all organizations are going to feel this way, and we certainly don't want to make that a requirement for NHIN Direct. But the question was whether, if an organization like an IDN or whatever wanted to say that we will turn away at the door without ever even excepting the message, decrypting it, and processing it to realize that it's noncompliant, if I want to, I would – if they choose to have a policy that basically says I want to be able to turn away at the door, at the gate any message that does not contain like a compliance C32 CTV whether this messaging approach could permit that or not. There was some discussion about whether that was a real policy … or not and the complexities of whether there is liability or isn't actually liability, I think, does raise to the policy level.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If I could suggest one other topic, Arien, do we have a term we're using for things necessary for the original go live versus what might be required at a larger scale? It strikes me that the assumptions of not having a full ability to look up another provider, but having to know where the provider is through external means represents what was perceived to be a shortcut to the earliest test implementations, but I think we need a way to at least state which is in which category and verify our assumption in that regard.

Arien Malec – RelayHealth – VP, Product Management
Right. What's the minimal set of technology and policy? What's the minimal technology and policy framework that needs to be in place for participating with confidence?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. I think the general sense is that because there is a target in the minds of the developers of actually using this, at least in some limited context, they are paying a lot more attention to both technology and policy issues than they would if the end of the project were a demonstration without PHI. And we want to both keep that in mind, use whatever simplifying assumption we can to get there, but not go beyond the bounds of a reasonable set of simplifying assumptions, and we could use some guidance. We need some guidance to discuss issues on the two levels of what makes sense for an initial limited implementation, or what makes sense to scale.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I think this gets to the point Arien was raising that assuming that there is the need for federal oversight over organizations that provide some or all of these functions, individually or together, those federal oversights and vetting of those organizations establishing through rulemaking a mechanism for that would take some time. What is the interim process for allowing everything from the pilots to initial real world implementations that are necessary for the prototyping in the meantime?

David Lansky – Pacific Business Group on Health – President & CEO
First, let me thank Arien for making the time today and taking the thoughtful trouble to go through all this with us and get us caught up. I think we can turn our attention to the material Mariann prepared. It'll

surface these issues, and some of them won't be reflected in this material, which is good. I think we have to start improving our master list, as Farzad just started to, of what should be on our radar, and then we need a work plan to start tackling these things … some guidance for everyone's benefit, for the policy committee to understand what issues are surfacing.

Mariann, what I'd like to do is go through your materials in not too – try to get an overview of it relatively quickly, and then come back through it again and look at it in more detail. But I think the overview will, itself, surface some questions about, just as this discussion has, whether the structure of our way of analyzing and thinking about these issues is meeting our needs or whether we need to come back to a larger framework. I think the challenge for me is there are many, many issues that we've already heard today that are triggered by any of these transactions, and I want to make sure we are comprehensive and systematic in our thinking about them, so I know we've got a path at that from the material you've got today.

Also, one other contextual thing: I guess it's a year and a half ago now ONC released a high level framework for privacy and security. That, in turn, builds upon the fair information practices and other frameworks that have been surfacing of a while. I think we need to do an exercise where we make sure that we are testing these modules like the one Arien just described against what ONC and others have articulated as the key criteria for addressing the policy concerns with information use. And I know we've just informally started doing that in the last half-hour. I think we need a process. We can come back to what the process is to make sure we do that carefully. With that introduction, can we go to the next set of slides? Mariann, can you take us through the material?

Mariann Yeager – NHIN – Policy and Governance Lead

Certainly, David. Thank you. If we want to maybe start on slide three, I think that we did want to provide a brief update on the status of the HIE trust framework. I think the group knows that there were a set of draft recommendations and other information and findings that were presented to the HIT Policy Committee on April 21st. I believe the feedback from the policy committee was positive on that front, so we are preparing the recommendation letter that would go to ONC from the policy committee, and we'll be circulating it to David and the group here for comment. I just wanted to make sure that you all understood and knew the status of that.

Then I think what the group had teed up to go through next was to walk through each of the five elements in the HIE trust framework in a little bit more detail, and so the first item that was teed up is the first element in the trust framework, which was discussing the agreed upon business policy and legal requirements and expectations. Then the other topic, I believe, will be addressed in other future meetings, for instance, the topic and teeing up the discussion around governance. It would certainly address the second element for transparent oversight, as well as enforcement and accountability.

There is a special interest group that's been organized that is teeing up the issue around identity assurance. There's a lot going on in that space, and so we are doing some legwork on that front to make sure that this activity is actually coordinated appropriately with some other larger context initiatives, and so we'll be working on that further on bringing that topic forward to the group. Then, of course, the minimal technical requirements are being explored as part of the project, the Direct project itself.

Going down to slide five is really where we start to drill down into the first element of the HIE trust framework. What we tried to do was to prepare some information based on work that's been done to date. This was not intended to put forward a particular policy framework, but to really start at a very high level with some basic assumptions and to help scope the policy discussion and to sort of set a context for some of the known factors, some of the issues at a high level that will require further discussion. This

group has certainly touched on a number of those very specific, granular level issues today. But we did want to sort of take a step back and make sure everybody was sort of on the same page and had a common understanding of some of the core assumptions that have been made around the NHIN to date and to look at that and how these things actually are implemented.

And so, one of the things we wanted to do, as we go down actually to slide six, is what was presented to the HIT Policy Committee. Those are sort of some high-level policy, business, legal requirements. The first I just want to highlight is that there is sort of an assumption that this group has made, I believe, to look to existing law as much as possible, but understanding that trying to identity where there may need to be further discussion about business policy, legal requirements in more depth, that may go above and beyond or more specificity than applicable law covers.

If we go to slide number seven, in talking about this with Arien, and I know that he shared this scenario with, I think, Deven. We thought it might be helpful to just sort of lay out sort of an existing scenario that really doesn't have anything to do with Direct necessarily, but to take a look at if we look at a scenario that's pretty common today, if we look at administrative transactions and lay out the flow of information and the types of mechanisms that are in place, we might use it as a point to sort of compare and contrast to the scenario that Direct is contemplated, and to maybe help frame some of these things.

In slide seven, in this example, again, this is just a sort of compare/contrast, providers today actually may use billing services, which a provider being a business associate and a billing service in this context is the business associate, to actually process his claims and queue those up and submit them to a clearinghouse, and those claims would be routed to a payer for adjudication. In this scenario, the contractural obligations are between the provider that's a covered entity and the billing service that they use, and the clearinghouse is the covered entity, and they also serve as a business associate to a payer, and they've, in that instance, on the backend of that transaction between the clearinghouse and the payer, that they are obligated to comply with law. That they are oftentimes have other obligations that they establish through contracts and different services that the clearinghouse could provide.

What we were trying to call out here is what obligations sort of exist today when billing services route transactions to a clearinghouse? In some instances, in this case, well, in all cases that each of those entities has to comply with applicable law. There oftentimes are contractual obligations, either between the billing service and the clearinghouse that the billing service actually has to certify or go through some testing or validation process before submitting to the clearinghouse.

In some instances, it's the provider and the vendor, and so there are different flows. But there is clearly, in most cases, an order for that transaction to flow between the clearinghouse, the billing service to the clearinghouse, there's some obligations that are established there. Today, they appear to largely be addressed through contracts or through the obligations that the parties have under existing law. And so that's just one scenario.

In looking at the Direct scenario and walking through … again, we're touching base routinely trying to kind of sketch out, find a way to talk about these issues to flush out the policy implications that similarly, now there doesn't appear to be a really wholesale different scenario, but we could actually apply some of the principles and the administrative transaction setting to this. In this instance, a provider, a lab, which is a covered entity, would use an intermediary. In this case, a HISP, which would likely, and the assumption here is likely be a business associate that would route the transactions to another HISP. In that instance, say, for example, it could be any number of different types of entities. It could be a business associate of the recipient of the information. Itself could be a covered entity itself, or it may not even be covered at all.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Actually, maybe we could advance the slides.

Mariann Yeager – NHIN – Policy and Governance Lead
This is slide eight.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Slide eight, yes.

Mariann Yeager – NHIN – Policy and Governance Lead
Sorry. My apologies. Thank you. In this instance, much like the administrative transaction scenario, that there are contractual obligations between the provider and sending the information…. There are likely obligations on the backend of this between the HISP that's routing it to the recipient to both comply with applicable law and likely contractual requirements there. The question is again the same. What are the obligations between the two HISP, and is applicable law sufficient to cover that relationship should there … how are certain issues, basically, and what are the responsibilities for privacy and security?

For example, one of the issues we walked through is who is responsible if there's a breach? Do those parties have an obligation to each other if there's a breach? For example, if there's a breach for the HISP that is sending it, I guess HISP A in this case, we know that there are obligations to the provider, as a business associate. If the breach occurs with the HISP routing it to the provider or pharmacy on the recipient side, do they have obligations to the other HISP? This is just a way to kind of lay out very simply a question and a context for the information that will be walked through.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
One thing that is not in this section, I think, or maybe it is, in terms of the business policy and legal requirements. But another assumption that we have on the governance and oversight is that both HISP are accountable to a regulatory third party and that there could be trust between HISP because kind of the transit of property because they both have been deemed as part of – they've been organizationally vetted, and they have accountability and oversight through a third party that's also being, I think, discussed in governance portion in steps two and three.

Mariann Yeager – NHIN – Policy and Governance Lead
In the absence, if we talk about an interim approach, I think that what this calls out is how would those obligations and that trust be addressed on an interim basis, and we have seen another NHIN scenario that that's been sort of addressed through contracts and other mechanisms on an interim basis. And so it just sort of helps call that out. In slide nine—

David Lansky – Pacific Business Group on Health – President & CEO
Mariann, before you go on, sorry to be slow on the uptake.

Mariann Yeager – NHIN – Policy and Governance Lead
No, that's fine.

David Lansky – Pacific Business Group on Health – President & CEO
I'm back to the previous discussion with Arien about what the HISP functions are in terms of the PHI content being sent in this payload. As we said in the earlier discussion, if it's essentially just the DNS server, then it's not having – the policy implications of having access to any of the PHI obviously scales up the certification of the HISP by some third party that Farzad just described. And I'm a little confused about, very confused about what functions these two HISP are playing in terms of having access to PHI.

Mariann Yeager – NHIN – Policy and Governance Lead
This is information we actually didn't tee up for this group, but some of the analysis that Arien has been doing is walking through a couple different scenarios that explore different levels of exposure that a HISP could have to PHI. It does vary.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
That's a really good point, David. You're saying that if in the conduct … the case we talked about so far is where the HISP do not perform functions that require them, whether it's transformation, for example, that would require them to have access to the payload.

David Lansky – Pacific Business Group on Health – President & CEO
Right.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
The cases that we've discussed, and I think Mariann, in slide two, explicitly says if there are, if the HISP does have access to PHI, then that opens lots of other issues and that this workgroup, as well as the privacy and security workgroup, has yet to address those.

Mariann Yeager – NHIN – Policy and Governance Lead
Right.

David Lansky – Pacific Business Group on Health – President & CEO
I was going to ask the reverse question. Is it a policy statement that the HISP don't have access to PHI, that they are just addressing service, or do they? If so, then the burden of establishing their trustworthiness seems to go up.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes.

John Blair – Tacanic IPA – President & CEO
This is John. Can I ask a question, David?

David Lansky – Pacific Business Group on Health – President & CEO
Sure, please.

John Blair – Tacanic IPA – President & CEO
When you're talking about access to PHI, can we just get a little definition there whether that means that they can look at PHI, hold PHI, or something like that versus whether they're just transporting PHI?

Mariann Yeager – NHIN – Policy and Governance Lead
In the scenarios that we walk through, technically I think they're talking about not requiring exposure to PHI for the purpose of routing. But when we walk through the practicalities of how this would be implemented, and this is teeing up directly for this group, realize that it could vary depending upon the services that the HISP provide. There may be some HISP that all they do is just route along. They don't open the packet. They have no need to do so. It became evident, however, that in many, many instances, and possibly in most instances, they would have a need.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
The way I would put it is we have identified a policy bound here, which is the architecture can enable, should enable, must enable the charge to the NHIN Direct workgroup and the Direct technical team is

built in such a way that the routing HISP doesn't need to look in the payload. That it doesn't need, doesn't require any access to PHI.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Farzad, excuse me. I think that it would be good to, at this point, define what access is, as was requested.

M
Yes.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Being able to read it, being able to see it, so if they are transporting a payload, you encrypt it.

John Blair – Tacanic IPA – President & CEO
David, to that, do you consider transporting when you're not looking at it or holding it still access? That is what I was asking.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
It's not, according to the breach rule so far. Even if it's divulged, but it's encrypted, it's not considered a breach.

David Lansky – Pacific Business Group on Health – President & CEO
I guess I'm interested less in sort of the legalisms at this point and anticipating possible consequences of this network being in place six months from now and us being ahead of the curve on the possible problems that could emerge.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If I could suggest that….

David Lansky – Pacific Business Group on Health – President & CEO
I think access of any kind creates the opportunity for either inadvertent or mischievous behavior that we have to be sensitive to.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If I could suggest that the assumption that the payload or the portion of the payload that contains any protected health information is encrypted is certainly consistent with HIPAA. That is, it's consistent with the requirement, as stated in HIPAA. It is an approach that is currently used widely to send protected health information in many contexts. That doesn't mean that it's right or that it is ultimately the best protection available, but it does mean that it's a compromise that's working in the industry. And as far as I know, I've never heard of a breach that involved decrypting encrypted information sent over the Internet using the technologies that we're talking about.

David Lansky – Pacific Business Group on Health – President & CEO
Wes, is that something that from a vendor and sort of routine operational point of view of a typical EHR, we can reasonably expect?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, yes. This is the technology that you use to put in credit cards in Web sites. It's the technology that's used for transactions transmitted over the Internet between providers, clearinghouses, and payers under the core guidance. There's….

David Lansky – Pacific Business Group on Health – President & CEO
I was more asking … I understood NHIN Direct to be a kind of simple … that something could be done between less sophisticated platforms, and whether the current vendor, you know, your typical EHR vendor out there today is now capable of transmitting an encrypted message consistent with this set of possible expectations.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I want to just say yes because I think it's true, but I'm trying to be careful not to let my enthusiasm run away with me here. At a minimum, I would have to make the claim that with the open source resources anticipated that many vendors can do this and do do this now. But when you get to the hundreds of vendors that represent the long tail of the curve of EHR vendors, it's possible that some of them would benefit by the open source resources that would become a part of available to them through this project.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I think what I'm hearing, Wes, is a concern. I think it's completely well placed, that there could be other business advantages or reasons or convenience to having access to the payload. And that unless there are higher requirements, as are appropriate for HISP that would not only merely route an encrypted payload, but would also want to have access to the payload, again, whether for convenience purposes or whether there are other benefits to them, advantages to them of that, that we need to not only move forward with NHIN Direct to enable the former group, which is merely doing the routing, but also to – I think this is more on the policy side – to establish what the higher level of organizational vetting would be required should the HISP choose to not only do the secure routing without having access to PHI, but also to have access to PHI. I think that that's completely right, and I think it's on the privacy and security workgroup and the NHIN workgroup to define what those are.

What we have so far articulated, it is feasible and perhaps desirable to have this in such a way that the payload need not be broached. But the question is, given the way it's happening today or there may be business interests in some of the likely HISP who would choose to do so and what can we say about that.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
That's exactly….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Very well stated. I would just add the concern that, to the extent the policy committee can, we enable that to be an operational decision rather than preordained in the sense that if we raise the requirements for all HISP—

Leslie Harris – Center for Democracy & Technology – President & CEO
Hello?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Hello?

Leslie Harris – Center for Democracy & Technology – President & CEO
I'm sorry. Something happened with my phone.

M
Leslie.

Leslie Harris – Center for Democracy & Technology – President & CEO
I'm sorry. New phone line.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If we raise the level of requirements for all HISP to the maximum level provided for the maximum services, then we've sort of defeated the attempts to….

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
We end up back where we started.

Leslie Harris – Center for Democracy & Technology – President & CEO
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's right. Yes.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I think that's exactly the point, Farzad, that you were making, which is to say there are ways to get at that with policy. Again, it's so analogous to the conversation we just had previously about identity. There are ways to get around that with policy that don't require you to increase technical complexity in order to accomplish the goal.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Right. I think, from a technical side, it's hard to make it simple, right? And I think we have succeeded, or I have hope that the technical team will succeed in building an architecture that enables the secure routing without needing to have access to PHI. I think that hard work from the technical side then enables policies that, say, that if you want to only do this, and you're not having access to PHI, you have to jump this high, not that high. But if you do want to have access to PHI, then you need to jump this high and that, I think, would have the affect….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
That's right.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
That's right. Now only of protecting the public in engendering trust, but also, frankly, of encouraging organizations to think clearly about whether they really need access to the data in accordance to some of the fair information practice principles.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
That's exactly right, and I think that's exactly the reason why this has to be – this conversation has to happen in a way that looks broadly at what might happen because just because you're saying it should happen this way, there are other scenarios that I think need to be considered from a policy perspective.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes. I would say that we should maybe fast track this specific issue for not only our workgroup, but also the privacy and security workgroup to consider. This goes beyond, frankly, NHIN Direct. This goes to all the organizations that receive information for operations purposes and re-disclose that information potentially to other organizations for operations purposes and that exchange that I think contributes to the lack of public trust that they know what's happening with their health information, has control over it. It's a broader issue than just NHIN Direct, and I think it's entirely appropriate for us to ask, I think, the privacy and security workgroup to put this on the fast track for consideration.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
The privacy….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Can I just ask a clarifying question? When you say no access to PHI from a technical perspective, are you also referring to no access to data type?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
What the architecture currently has is as an e-mail message in the header, it just says what the file type is or what application is expected to open it. It doesn't specify, for example, that this is a laboratory result or … result.

Joy Pritts – ONC – Chief Privacy Officer
...or….

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner

Yes.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Okay. Or a CCR or something like that.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
It could say it's a CCD if it's specified. You know, open this up with a CCD reader or whatever. Joy, did I misspeak or speak too soon about privacy and security workgroup taking this on?

Joy Pritts – ONC – Chief Privacy Officer
The privacy and security workgroup has started to look at factors that may require additional protections such as the ability to view PHI through an intermediary, and so they've already started to look at that, which I think is good, to align with this workgroup a little bit better. But I think we also need to talk about coordinating schedules of both of the workgroups or perhaps having joint sessions so that the work is addressed by both simultaneously.

The NHIN workgroup, this workgroup is on a different schedule than the privacy and security workgroup. This workgroup is expedited, and privacy and security right now meets, I think, once a month.

David Lansky – Pacific Business Group on Health – President & CEO
It sounds like we need to come up with a to-do list, a work plan, and then divide up where we can some of the appropriate places for the conversations to happen and try to consolidate our results, so the policy committee gets a consistent view.

Joy Pritts – ONC – Chief Privacy Officer
Yes, and because it should be a consistent view, I think it would be good to have a kind of combined workgroup perhaps maybe or something of that nature so that the privacy and security workgroup is actually kind of integrated with this workgroup, at least for some of these issues.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. I agree with that. I don't know what process ONC has in mind, but I made this point at the standards committee meeting also. The standards committee also has a privacy and security workgroup, and between these three workgroups, it just seems like, especially because of the time pressures right now, it would be good to apply those resources together and coordinate it.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
We'll take this on as an action item to figure out what the best process would be for considering the issue of the broader issue, I think, of the organizations that, in the course of providing a service, have access to PHI and what they do with that. I think it's a broad issue. The specific example of that is when those organizations are enabling organizations for secure routing. If they choose to use that as an opportunity to provide other services that either require them to have access to the payload, or they choose to implement it in such a way that de facto beats them to have access to an encrypted PHI, what the additional requirements would be for those organizations, whether from a policy side or potentially even legally in order to make sure that there's public trust. So we will take that, and Joy and I will try to figure out a plan.

John Blair – Tacanic IPA – President & CEO
Farzad, this is John again. I've got to push this a little further just to make sure that everybody is on the same page. On this access question, if the entity is just transporting, not looking at it, not doing anything with it, and I guess I'll ask David. Do you still consider that access if the entity is responsible for the transport?

David Lansky – Pacific Business Group on Health – President & CEO
Mike concern is capabilities and functions, not what they do, but what they can do, and what enforcement or controls or policy mechanisms we have around that.

Leslie Harris – Center for Democracy & Technology – President & CEO
David, this is Leslie. Can I ask a question? We looked at slide seven, which showed us the transfers of data now. There's transport there. Do we have rules for the transport in those situations?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
That was my point, Leslie, was that in the existing world this is a real issue, as you well know, much more broadly in terms of what organizations can do with information they have access to.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
But I think this is a different issue now because this is happening with public funds and with government sanctioned trust enabling….

Leslie Harris – Center for Democracy & Technology – President & CEO
I don't disagree. I'm just curious as to what the experience, plus it's just the scale of this is going to be enormous.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I don't think this happens, you know, health information exchange is not robust now, to say the least, right?

Leslie Harris – Center for Democracy & Technology – President & CEO
Right.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I think the issue is to really think about what it means, as you say, once this is really scaled up.

Leslie Harris – Center for Democracy & Technology – President & CEO
And I do think it's about for transport, pure transport. I don't think it's about – I think it's about – I do think it's about capability and what they aren't allowed to do.

David Lansky – Pacific Business Group on Health – President & CEO
John, can I ask you? I'm guessing you're asking this question and pressing on it because you've got some experience in New York that we should hear about. What are you getting at?

John Blair – Tacanic IPA – President & CEO
No. I'm actually not pulling off of experience here or anything like that. I just think that there are two different things being said here. I just want everybody to get on the same page on the definition. I think we're fine once we do. But I think that there are some that feel that even, and this has nothing to do with experience. This is just in these different committees and listening. I think there are some that feel that even if you're not looking at it, even if you're not holding it, if you are just transporting it, that is access to it, and that's kind of what I thought I heard you saying, David, that even if the organization is not looking at it, not opening it, but if they have access to it, there's potential for mischief, and we need to think about that versus whether you open up and look at it and then read it and call that access. I just want to make sure we have the right definition. We can deal with it however we choose.

David Lansky – Pacific Business Group on Health – President & CEO
Right.

Joy Pritts – ONC – Chief Privacy Officer
This is Joy, and I think what you've raised as an issue is that you're taking the overall issue, I would say, back a step. It's not just, you're looking at functionally whether the "intermediary" could possibly unencrypt the information or decrypt the information and have what we would traditionally call access to as the first step. Then on top of that, he next step you would look at is, all right, what if – but they're not supposed to under the agreement.

John Blair – Tacanic IPA – President & CEO

Right.

Joy Pritts – ONC – Chief Privacy Officer
Then the next thing you would look at is whether they are supposed to be doing that under their business model.

John Blair – Tacanic IPA – President & CEO
Exactly right, yes. Even if you're not going to call it access, whatever you call it, if they're transporting it, there have to be some requirements around that to further give trust, confidence, and assurances. Then if you … part of your function is to open it and do things with it, that's a second thing.

Joy Pritts – ONC – Chief Privacy Officer
Right.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
That's been happening for many years in the billing industry where they actually do have a set of policies that are informal or somewhat formal, and if we do speak with Emdeon or some of the others, we may be able to just learn about what some of those service level agreements look like because there are those kinds of requirements and responsibilities, obviously, for transporting this kind of information without actually inspecting the payload.

Joy Pritts – ONC – Chief Privacy Officer
That's basically what my question was, not necessarily that these should be the same, but were they operating with any rules on transport?

David Lansky – Pacific Business Group on Health – President & CEO
Right, and I think NEHIN and UHIN in Utah and Massachusetts also have a similar set of rules for the claims that they transact and the eligibility transactions that they do.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Right. UHIN is a transportation mechanism. They do not inspect payload. I'm not sure about NEHIN.

David Lansky – Pacific Business Group on Health – President & CEO
Right, the same with NEHIN.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Right.

John Blair – Tacanic IPA – President & CEO
I'm just trying to get at the definition because some would say if you're transporting that you have access. We're using access differently. I just want to make sure that everybody is speaking the same language.

Joy Pritts – ONC – Chief Privacy Officer
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That would be an early part of this activity would be to either clarify and decide on one or distinguish the two cases and deal with them.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Agreed.

David Lansky – Pacific Business Group on Health – President & CEO

Let's, Mariann, if you want to go back to your slides and keep us moving forward, that would be helpful.

Mariann Yeager – NHIN – Policy and Governance Lead
I'm wondering, just to get a read from the group, it sounds like there have been two clear distinctions made. Really the rest of the information had presumed that these HISP could elect to take on additional and do additional services above and beyond just routing of encrypted information. The question is, is there value in kind of going through the rest of those, or should we really take a step back and really revisit the process for approaching this jointly across a couple workgroups or just trying to get a read from the group in terms of processes, and to be respectful of your time.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes, I agree with Mariann that the way that this was drafted, a lot of these like the breach example is assuming that high case where the HISP doesn't just do secure routing, but they also potentially have access to the PHI. I do think that maybe it would be better to have a broader set of input to make sure that we're looking at this with a wide enough lens than just the NHIN Direct example here.

Mariann Yeager – NHIN – Policy and Governance Lead
David, what's your thought on that, or would you like to do just a high level walkthrough just to orient the group, or would you prefer to take a look at the process and then bring together a joint group?

David Lansky – Pacific Business Group on Health – President & CEO
I think it's worth taking five or ten minutes and go through the structure and categories you have, so everyone can just understand where you're going. Then just have some high level reactions, not get into the detailed policy implications.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes. If we do that, I just want to make sure the group appreciates that we are – this does not represent in any way us trying to short circuit the discussion that does need to happen. This is some very preliminary thinking.

David Lansky – Pacific Business Group on Health – President & CEO
Yes. I'd like to go back to the point I made earlier and, as we think about this reconvening and reassigning the work to these groups, go back to the question of the overall framework. What we'll see here in a second is about 12 categories of issues that surface. And, as we've seen today in this discussion, it'll be helpful to organize these categories within some of the, I don't know, I'll say traditional groupings of issues that we've already verbally been surfacing ourselves. Maybe, as you just tick these off, Mariann, the group as a whole can think about what's the best way to organize this discussion going forward. Why don't you go ahead and walk us through the categories you've got?

Mariann Yeager – NHIN – Policy and Governance Lead
Certainly.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Sorry, just to clarify, these are all, I think, thought to be under that very first bucket in the trust framework, which is business policy and legal expectations.

David Lansky – Pacific Business Group on Health – President & CEO
And it's worth noting that our discussion today has gone outside of that first bucket, as we talk about the identity assurances and other categories too. The other thing I want to mention from the last discussion, it strikes me that in our, whatever it is, third big bucket on monitoring and enforcement. That's sort of an implicit question mark for me in the whole discussion we've had this morning.

How would these potential, whether we call them mischief or inadvertent behavior of the transport or otherwise performing HISP, how would we know if some kind of unacceptable or unexpected behavior is going on, which is the monitoring function? Then who is, if we are operating outside of a business associate agreement, what's the enforcement mechanism that would come into play? We should keep

that in the back of our mind, as we think about which policies we think are the constraints on behavior. Go ahead, Mariann.

Mariann Yeager – NHIN – Policy and Governance Lead
Certainly. Thank you again. Just walking through these, and there were some questions when we first distributed the materials about sort of how these topics came about, and so there have been work just over the past number of years. I think you all know, in taking a look at what sorts of issues and mechanisms might need to be in place for health information exchange for the NHIN broadly, not specific to the Direct scenario that this group is focusing on, but just more broadly across a wide range of comprehensive functions. So we'll sort of draw on that as some examples. But what we found as beneficial is to kind of have a sense of to what extent you can rely to applicable law and where there may be areas where it's unclear how those obligations for trust could be implemented to support it, and so this is just really to kind of help more for scoping, but not to presume any particular frame or for any particular outcome, but to just scope the assumptions around it.

The first item and the second item and third item really have to do with privacy and security obligations and really purposes for which data are exchanged. And so for privacy and security, as an example, the assumption here would be that there clearly is a legal requirement that entities are abide by law that apply to them, and federal entities, as an example. This would include the FISMA and covered entities, if they're covered entities if they're subject to HIPAA. Then if a participant is a business associate, that there are also contractual obligations to apply to comply with that.

The question that came to light over the past years is there could actually be folks involved, participants involved in the exchange that are not federal entities. They're not covered entities or business associates. The question then was what were rule would govern what they do, and so for the NHIN exchange, the way that was addressed, and that is again, it was not necessarily a gap, but it was circumstances that they had to deal with is that they were able to address that by requiring HIPAA, certain HIPAA provisions for privacy and security, the contractual standard of performance, and that there were certain requirements that participants would have to make sure that there were appropriate policies and procedures in place with their users and technology partners to make sure that that indeed were carried forward.

The question, and again, I think that I don't know if we need to tee up the direction necessarily for Direct, but it does beg the question of what is really required above and beyond existing law to assure that data are adequately protected, and I think the group touched on some of those topics today. We talked previously about identity assurance, etc. Are there gaps or issues that need to be addressed to assure adequate trust? I think that's the issue the group had sort of tabled and will explore further.

The second and third items also point to what's done with the data, and the NHIN requirement that's in place today is that information would be exchanged based upon HIPAA permitted purposes and those contemplated for meaningful use. With the NHIN exchange, because it's in the early stages of implementation and production, that they took a more conservative approach, and they'll only – currently they further constrained it to a more narrow set of permitted purposed, and we'll broaden that on a case-by-case basis, and that was in the interest of not being overly broad in its uses, but to take a step-wise approach and incrementally address it over time. And so the question for Direct is what should be really the policy statement around uses and disclosures of the information, not just for the purpose of the exchange, but also what happens to the data once it's received.

On that note, the third item has to do with future use of data received through from NHIN participants. This expectation basically says that once data are received and integrated into a user's system that they could be basically used or disclosed as any other information that's held in its records and retained and protected, both in accordance with applicable law, as well as local policies for data retention, and so that's a pretty significant assumption and that it does really link again to existing law and local policies around that.

We want to move on to slide 11. The item, the element….

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Mariann?

Mariann Yeager – NHIN – Policy and Governance Lead
Yes.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
What is the purpose of this row? Is it to say? I guess I'm struggling to know what to make of existing law or the assertions here, as based on the previous conversation we had, there are lots of questions about what the "it" is.

Mariann Yeager – NHIN – Policy and Governance Lead
Carol, were you asking about a particular item or just in general?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Privacy and security.

Mariann Yeager – NHIN – Policy and Governance Lead
There were, and I'm not sure I'm following your question. Were you asking why it's important to articulate kind of how or why applicable law exists?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. I'm asking what is the intent behind saying this is an NHIN requirement. Is it to say that this is a requirement, a basic requirement, or is the intent is there are no other requirements…?

Mariann Yeager – NHIN – Policy and Governance Lead
I think it was to identity the basic requirements and to use this as a way to identify whether that's really covered the bases, essentially.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. The only thing I would say, even for things that you consider to be covered under existing or applicable law is that I think it is also part of the NHIN work to clarify the policy expectations for how that law is applied or the technology expectations for that matter. In other words, it may not be a question of saying, you know, citing particular laws, but it may be a question, as you know, in many of these laws, a lot of these things are not really clearly articulated in terms of how they might apply to health information exchange. I do think, even where there are existing laws, it's important to think about that as part of the scope here.

Mariann Yeager – NHIN – Policy and Governance Lead
Right.

Joy Pritts – ONC – Chief Privacy Officer
Carol, this is Joy. I think that's right, but I also – it's my understanding, Mariann, correct me if I'm wrong, that what this was intended to, at least as a DURSA, was to set a very minimal standard for participation, which was they expected participants to actually comply with existing federal and state law. So it was more about, if you aren't even complying with those, you're not going to – we're not going to allow you to participate.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
And now that you clarify these are some of the things from the DURSA, that makes a lot more sense. I just….

Joy Pritts – ONC – Chief Privacy Officer
Before we accept that clarification, is that right, Mariann?

Mariann Yeager – NHIN – Policy and Governance Lead
That isn't. It's really not just about the legal agreement, but there are also, and because we're covering this at such a high level, there actually were other specific obligations that were, there were more detailed policy and technical expectations. The technical requirements addressed in the specifications and other things around auditing and breach reporting and other things that they felt were necessary to call out.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If I could add a thought here, in playing out the technological requirements versus policy issue, which is the interface that we're talking about here a lot, previous work based on a broader set of functions led to a set of standards that conveys the policy of how the data will be used in actual explicit metadata sent along with the data creating a significant barrier to implementation for the recipients of the data. They had to now build new machinery to retain and interpret that metadata. We're hoping to find sort of the right place to slice the balance of functionality such that new functional complexities associated with the software that deals with the receiving data are not overwhelming or perhaps not even whelming.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes. I would just hope that we don't end up back where we started, that we can define a policy, a narrower set of policy bounds and situations. That our hope when we started this, and I'm a still a strong believer in the possibility of this is that we don't end up in a situation where in order to be able to send information from anyone to anyone, you need to essentially have the equivalent of the DURSA because we know that that's going to be a heavy threshold to cross for many organizations that are less read into the assumptions there.

Mariann Yeager – NHIN – Policy and Governance Lead
This is very helpful, and I think that this is helping to call out at what point the sort of trigger activities occur. Are there any questions further about one, two, and three? We'll move on to slide 11, and this slide addresses the legal requirements for obtaining consent or authorization for treatment purposes and for authorizations, and so the assumptions here of that and all NHIN scenarios that the sending entity, this is the party that sends a request for information or that simply transmits information as to make sure that it has met its applicable laws and regulations before exposing data, and that means before sending that information or making a request that they obtain consent or authorization if one is required for treatment purposes before doing so, and that would be abiding by the laws and regulations that apply to that entity.

Similarly, if there is a request for information, then the party that responds to that request and releases the information is responsible for meeting its own legal requirements, and that would mean that if there's consent or authorization required for treatment purposes, for instance, in that state, that they would indeed be responsible for obtaining that, and that was a pretty important assumption to avoid putting burden on the party requesting the information where they may be in a different jurisdiction or subject to a different body of law from having to apply with a whole other set of legal requirements outside of their jurisdiction. And so the question then was what would be for Direct. This is a topic that would be teed up for future consideration is what are the obligations of HISP, the recipients of data around consent or authorization if any?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I believe this one where the privacy and security workgroup had very quickly identified the caveat that this depends on whether the enabling HISP has access to information or not.

Mariann Yeager – NHIN – Policy and Governance Lead
Right. Exactly.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
And if they don't, it's a different situation than if they do.

Mariann Yeager – NHIN – Policy and Governance Lead

Exactly. Similarly, for authorizations, to release information that if there is a request for information that requires an authorization, that that request would be sent along with – that the authorization would be sent along with the request. And so, in this instance, for Direct, would it ever be necessary to send along a copy of an authorization with the information that's being transmitted, and what, if any, implications would there be to HISP. That was just a question that may … narrow set of circumstances, it may never apply. But it was just…. Any questions about four or five?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
This is Farzad. On five, again, we're matching through a set of issues that were teed up for NHIN exchange in particular, and asking in some ways things like the responding participant. It assumes a query and response model, although I will say that one can think of and must, should think of extensions of the NHIN Direct model to cases, as Wes has put it, where you have paired pushes, like a 270, 271 where two pushes start to look an awful lot like a query.

Mariann Yeager – NHIN – Policy and Governance Lead
Right. Exactly. These are sort of the working set of assumptions that are in place today, and some of these may apply, you know, sort of across the board for all NHIN scenarios and also trying to call out….

Looking at six, seven, and eight, I think item number six is the local autonomy principle. I think this group has talked about this at some length. It was part of your prior set of recommendations. I don't think there's any question. I don't think that – the assumption is that a participant would apply their local policies to determine when to send data essentially for the Direct scenario.

There is, in number seven, in the NHIN exchange scenario when there are requests for information that, or when sending data, that there's some expectations of conformance with a set of specifications and testing requirements….

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Right. David, this would fit under number five of our big buckets, probably.

Mariann Yeager – NHIN – Policy and Governance Lead
Right. The technical requirements, right, and so to, you know, what sort of level of understanding does there need to be to make sure that's in place. In duty to respond, this is an area that this is actually a pretty meaty topic when you're looking at making sure that there are really that there's comprehensive data that are available for treatment purposes that if a participant is going to request data for treatment purposes, that they also have a duty to respond to requests for treatment purposes. They can determine whether or not to release the information based on whatever law and local policies. There's a reciprocal duty there, so that conceptually this is more a business rule, and if there's any sort of reciprocal duty to participate in Direct, it should apply. In other words, if somebody is sending data to a provider, should that recipient….

Looking at nine and ten, this has to do with really looking at some of the requirements around participant obligations and responsibilities around breach notification or addressing with dispute. Here is an area where clearly applicable law plays a role. But the question is, are there responsibilities or duties between the participants or HISP to address breach notification? I think we've talked about this. That depends. If the HISP really has no access at all to PHI, then clearly it's a totally different scenario where they might. And around disputes, how would disputes, if any, be addressed? And should there be a consistent process across participants or not?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Mariann, if the HISP, which is just doing the routing, let's say, sends it to the wrong recipient, doesn't that trigger this issue?

Mariann Yeager – NHIN – Policy and Governance Lead
It likely could, but it depends.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Joy, you could probably speak more to when the breach notification or the determination of breach kicks in, in the instance where the data is encrypted.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. Actually, my point wasn't to actually get into the sort of specifics of how this would work, but I was just reacting to Mariann's comment that if they're not looking at PHI, then breach doesn't apply.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Well if they can't … I think the issue is if they can't look at PHI, i.e. the payload is encrypted, then they send it to the – even if they send it to the wrong person, then I think, according to current law, and I would think consumer expectation as well, there hasn't been a breach.

Leslie Harris – Center for Democracy & Technology – President & CEO
But there may be other liability, right?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I don't know.

Leslie Harris – Center for Democracy & Technology – President & CEO
I don't know.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
You know better than I do what the situation is if encrypted data gets sent to the wrong place.

Leslie Harris – Center for Democracy & Technology – President & CEO
Yes, but if it … it's less – you can look at it, but that the original party that needed it didn't get it.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I see. You're saying the….

Leslie Harris – Center for Democracy & Technology – President & CEO
I'm not talking about breach laws.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I get you. This is more in terms of the … whether it got to where it needed to go for treatment purposes.

Joy Pritts – ONC – Chief Privacy Officer
It's more like torte liability.

Leslie Harris – Center for Democracy & Technology – President & CEO
Yes, it is, isn't it? I don't know whether that's our story about this. I assume that there'll be plenty of lawyers coming up with a policy when it happens, but….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we have to examine that. We sort of have a body of experience around the fax machine where there are both personal and technical failures to deliver information.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I was going to say, if all the faxes that were not delivered because they came to my personal home phone number are any indication.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, but I don't want to make a presumptive statement that the situation with fax would apply here, but simply make the point that we have a body of experience to look at in this regard, and we have the ability

to sort of examine the similarities and differences to faxes in this regard and use that as an approach to addressing the issue.

Jonah Frohlich – HIT at California HHS Agency – Deputy Secretary
Going back to the clearinghouse issue, having spent time working with payers, when packages don't get delivered that should be, and there's no response, and there's a black hole, there are all sorts of implications and issues that I think bring the question what is the right policy for this. I think, to some extent, we do need to examine what are the right policy considerations for mis-delivered mail or packages or faxes in this case.

Mariann Yeager – NHIN – Policy and Governance Lead
Great. I think that really kind of takes us through on slide 14 the considerations of risk and if there are, would ever be a need for legal agreements. I think this group has honed in on a couple key issues. I think the next steps really, based on what the group has talked about, would be to sort of come up with that joint process and approach for considering these issues and given multiple scenarios, one where … would have no ability to actively participate … circumstances where they might. David, that really kind of wraps up, at a high level, some of the considerations.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks a lot. Thank you for bringing up so muc material to get us started. It sounds like the next steps will be to convene a subgroup to talk about the multiple workgroups and how they can best tackle this against the master list, Mariann, that you'll give us based on today's conversation. Let me see if people in the workgroup have any other either process suggestions or substantive comments they want to make sure are on the radar for today.

Leslie Harris – Center for Democracy & Technology – President & CEO
This is Leslie. Can I just ask a question about this identity … what that work is because there's obviously technical work around identities, but identity providers have a host of complicated policy issues?

David Lansky – Pacific Business Group on Health – President & CEO
Mariann, can you go back … and catch us up on…?

Leslie Harris – Center for Democracy & Technology – President & CEO
I just want to understand who they are and how they fit in, and how we….

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes. This is Farzad. When we held the hearings … the message we got loud and clear was there's been a lot of work done on this already in the federal government. If you don't take advantage of that, we're going to find you and shoot you.

Leslie Harris – Center for Democracy & Technology – President & CEO
And I agree … and I agree with that. There's a lot been gone on about exchange inside the government.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
The first….

Leslie Harris – Center for Democracy & Technology – President & CEO
There's a lot more going on right now.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Yes. The first step for us was to, under Andrew McLaughlin's leadership, was to pull together folks in the federal government … to kind of generate at least a straw proposal around that initiative.

Leslie Harris – Center for Democracy & Technology – President & CEO
Okay.

David Lansky – Pacific Business Group on Health – President & CEO
Any other suggestions for our process or issues of policy you want to make sure are on this list? Hearing none, I think we've got a good overview today and dug in deep into a couple of topics, so we are in a good position to drive forward. Mariann, you'll help us sketch a process from here, and we'll circulate that to the group and get a subgroup involved in charting our work….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
At the risk of coming off mutely, can I say are we – there's obviously a tradeoff between when you want it done and when it can be done. Are we clear on – is there any need to be specific on timelines or anything like that as part of the process of making up the process, the net of process of making up the process here?

David Lansky – Pacific Business Group on Health – President & CEO
Well I guess I'm looking back to Arien's slide, at least as it pertains to the Direct component of this discussion. Wes or Farzad, do you have a better or more specific sense of timelines that are critical?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I think what we need to do with Arien is to highlight which of the policy issues that have been floated up are there, kind of technical developments that are dependent on them being clarified. And then to see whether there are, I think, then we can go one of two ways. One, see if we can quickly reach consensus from a policy perspective in terms of how to resolve those. Or, two, to say more complicated, build it in a way that ideally can accommodate multiple policy directions. One of the to-do items is to circle back with Arien and ask that specific question: in the technical development, are there branch points right now? I think we may have identified a couple in the course of the face-to-face meeting, and then further articulate it today that will come to play.

David Lansky – Pacific Business Group on Health – President & CEO
Okay. We'll just do that work on a staff level, I guess, and get the details. Any last words? If not, I think we will get the benefit of adjourning a little bit early.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Terrific.

Judy Sparrow – Office of the National Coordinator – Executive Director
David, we just have to check with the public to see if there are any comments.

David Lansky – Pacific Business Group on Health – President & CEO
Yes. Thank you, Judy.

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you see if anybody wishes to make a comment? While we're waiting, the next full NHIN workgroup call is June 15th. Any callers?

Operator
We have no questions at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Thank you, David.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you, everybody. Talk to you again soon.

Judy Sparrow – Office of the National Coordinator – Executive Director
Bye.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner

Bye.

Mariann Yeager – NHIN – Policy and Governance Lead
Bye-bye.

Public Comment Received During the Meeting

1. Under duties for respond...should NHIN direct then contain patient Consent information. Should the technology for the patient consent be at the individual provider level? If so what implications does that have for the technology? Hisp Directory? PKI?

2. Would not the identity of the sending organization provide specification of content to the HISP? In other words if data are sent from a mental health organization - would that not be known to the HISP?

3. If the HISP transports only encrypted PHI end to end....they wouldn't have anything. There should be no need for the HISP to interrogate / open the message (unless they are also offering clearinghouse services)...

4. PHIN MS actually does not require a "HISP" at all. Why is one needed here?

5. Payload (email vs. PHI docs). Is it fair to assume the HISP should be able to apply / vet the assurance requirements based on payload? I.e. email reqs digital signature vs. CCD requires certificate?

6. Is it fair to assume the HISP doesn't write the policy assurance guide but implements the policy as specified by a framework participant (i.e. a Physician's IPA)?

7. What if provider A doesn't know provider b but wants to look up related caregivers using patient as a primary key? It is envisioned that the HISP could offer these lookup services?

8. This description of NHIN Direct is exactly what the PHIN Messaging system is. The latter used ebXML, but what is the NHIN Direct project testing?

9. Comment to Carol's Questions...Intermediaries don't have to have PHI. They can simply serve to encrypt at POC, deliver and work with end recipient to decrypt. It is similar to PCI requirements of credit card industry - i.e. don't store off the CC information, send encrypted information across the wire for settlement to the banks. Merchants don't need the CC info nor should have it. Apply same policy to Intermediaries. Just an unsolicited thought.

10. What Routing Info is in HISP? How is identity of the receiving provider verified? If patient requests audit of who was sent their info - do they see the HISP routing info? If so how do they (patient) interpret HISP address?